ATTACHMENT A

SUBSTITUTE SPECIFICATION
(Including All Changes Made to the Specification in Published International Application No. PCT/SE2005/000233)

METHOD FOR AUTHORIZATION

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] The present invention concerns a method for granting access to restricted areas such as computers, doors, vehicles, or other areas to which access by a user is controlled.

DESCRIPTION OF THE RELATED ART

[0002] Computers and mobile telephones are currently used as equipment for carrying out transactions and for giving a signature of different types. Furthermore, computers are used to an ever greater degree to collect information with different degrees of confidentiality. It is often sufficient to log in with a password or a PIN code in order to subsequently be able to carry out transactions or to handle information during a limited period. That means that a terminal might be open for use by an unauthorized person if it is left unmonitored, or if it is stolen within a certain time from the time an authorized user logged in.

[0003] In order to prevent that, there are requirements for codes, or for the use of a magnetic card, or what is known as a "smart card" as a means of identification. One disadvantage of such systems is that the user often considers them as burdensome, and as a result often seeks to exploit shortcuts, which reduces the level of security.

[0004] One problem with codes is that they can be read by an eavesdropper unless the information has been encrypted, which can create a demand for particular software, hardware, or a password that is to be distributed such that it can be used by the user.

[0005] The present invention solves that problem and offers a method by which the identity of a user can be established with high security.

SUMMARY OF THE INVENTION

[0006] The present invention thus relates to a method for granting access to restricted areas such as computers, doors, vehicles, or other areas to which access by a user is desired to be controlled. The method includes the transmission of a code over a short-range radio link. An access code (an ID-code) is transmitted from a central computer using radio waves, to a radio terminal in the possession of the user. The radio terminal transmits the ID-code over the short-range radio link to the restricted area. A transmitter unit in the restricted area transmits the ID-code to the central computer, and the central computer compares the received code with the code that the central computer transmitted to the radio terminal.

BRIEF DESCRIPTION OF THE DRAWING

[0007] The invention will be described in more detail below in association with embodiments of the invention as shown in the attached drawing, wherein

[0008] Figure 1 shows a block diagram of embodiments of an access control system.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0009] The present invention thus concerns a method for granting access to restricted areas such as computers, doors, vehicles, or other areas to which it is desired that a user have access. The invention will be described below in association with an embodiment in which access to a computer is desired, and also an embodiment in which access to a locked door is desired. However, the invention can be utilized for other restricted areas to which it is desired to grant access, such as vehicles, telephones, etc.

[0010] The method includes the transmission to the restricted area of an ID-code over a short-range radio link.

[0011] According to the invention, an access code (an ID-code) is transmitted from a central computer 1 over radio waves to a radio terminal 3 in the possession of the user. The radio terminal can be, for example, and preferably is, a mobile telephone. It can, however, for certain applications be constituted by a communication radio of the type, for example, that is used by rescue services. For the example in which the radio terminal is a mobile telephone, the transmission takes place over a telephone network 8, via a base station 7, to the telephone 3 via radio link 9.

[0012] Furthermore, the radio terminal 3 transmits the ID-code over a short-range radio link 5 to the restricted area 2, as is illustrated by means of the arrow.

[0013] The restricted areas in the form of a computer 2, and a door 11, or a transmitter unit 4, 12 within the restricted area transmits the ID-code to the central computer 1 over a computer network 10.

[0014] The central computer 1 subsequently compares the code that has been received with the code that the central computer transmitted to the radio terminal 3.

[0015] A circuit has in that way been created in which a transmitted code can be compared with a received code. In the case that the codes agree with each other, the central computer 1 can, in the next stage, transmit a second code to the computer 2 that makes it possible for the computer to be used in the manner intended by the user.

[0016] Since the central computer 1 transmits an ID-code to a particular mobile telephone or other radio terminal 3, it can be assumed that the user of that mobile telephone is the person who transmits the ID-code to the computer 2 over the short-range radio link 5. Alternatively, the circuit can be used in such a manner that a comparison of whether the codes agree is made, which in that way can be assumed to specify that the correct person is using the computer, or that the use of the computer is unauthorized.

[0017] According to one preferred embodiment, the central computer 1 is initiated to transmit an ID-code to the radio terminal 3 as a result of either a transmitting device associated with the restricted area, or the radio terminal transmitting a request for a code to the central computer 1. With respect to the computer 2, the request can be transmitted over the computer network 6, 10, 15, or, with respect to a mobile telephone, over the mobile telephone network 7, 8, 9.

[0018] It is naturally possible to initiate the circuit at any freely chosen point, i.e., at the central computer 1, at the mobile telephone 3, or at the computer 2.

[0019] According to one preferred design, the short-range radio link 5 is what is known as an "RFID" link of known type. Such links work in two directions with two

transmitting units and two receiving units, or they can work in one direction only such that one unit transmits an inquiry signal that is received by, modulated by, and reflected by a second part in the form of a transponder. The ID-code can, for example, be transmitted in that manner by means of the modulation.

[0020] According to an alternative preferred embodiment, the short-range radio link 5 is what is known as a "Bluetooth" link.

[0021] The computer 2, or the door 11, and the radio terminal 3 have in both cases a transmitter/receiver unit 3, 4, and 3, 12, respectively for the short range radio link.

[0022] According to one preferred embodiment, the radio terminal 3 is a mobile telephone constituting one part of the short-range radio link. The radio terminal 3 is preferably a mobile telephone with an integral Bluetooth function.

[0023] A Bluetooth module is thus built into the computer 2, and the door 11. It is also possible to use another radio technology, such as WLAN (Wireless Local Area Network). However, it is important that the range of the radio link be made sufficiently short, independently of the technology used, in order to activate access to only the restricted areas that are intended.

[0024] According to one embodiment, the restricted area is a computer 2 or a computer terminal to which access is required.

[0025] In that embodiment, the user can request via the computer 2 a code from the central computer 1 in order to be able to use the computer 2. That request can contain the ID-code of the user. The central computer 1 thus transmits the code to the mobile telephone 3 of the user, which subsequently transmits the code over the short

range radio link 5 to the computer 2. The computer 2 transmits the code to the central computer 1. The central computer in that way receives confirmation that the correct code has been received by the computer 2, whereby the user can use the computer 2 in the manner that is granted by the code. That can be a question of full or limited use, such as carrying out financial transactions.

[0026] According to a second embodiment, the restricted area to which access is to be authorized is a door 11 or a gateway to which access is required so that it can be opened. In that case it is preferred that the restricted area includes a communicator 12 connected by a communications link to the central computer 1, which communicator 12 is arranged to communicate with the radio terminal 3 over a short distance using an RFID link or a Bluetooth link as short range radio link 13.

[0027] According to that second embodiment, it can be a question of rescue personnel being equipped with a radio terminal 3 in the form of a mobile telephone with an integral RFID link or a Bluetooth link as short range radio link 13. The communicator 12 is also equipped with such a link. When a fire-fighter, for example, wishes to open the door, he calls the central computer 1 over the telephone network 7, 8, 9 and transmits identifying information about the door that is concerned. The identifying information can be a numerical designation or another unique identifier.

[0028] Alternatively, the telephone 3 communicates through the short range link 13 with the communicator 12, whereby the number of the mobile telephone is transmitted to the communicator 12. In the latter case, the mobile telephone and door identifying information is transmitted from the communicator 12 to the central computer 1. In both cases, the central computer 1 subsequently transmits a code to the mobile

telephone 3 that, once it has received the code, transmits it to the communicator 12 over the short range link 13, whereupon the door can be opened.

[0029] It is clear, both in the case of a computer 2 and in the case of a door 11, that the code can vary with time when the central computer 1 transmits the code to the radio terminal 3 and to the respective restricted areas 2; 11. Variation in time makes unauthorized acquisition of the code through eavesdropping significantly more difficult.

[0030] According to one preferred embodiment the communicators associated with the restrictive areas 2; 11 can be configured to compare the codes received from the computer 1 and from the radio terminal 3.

[0031] According to one preferred embodiment, the code transmitted to the central computer 1 includes a network address belonging to the respective restricted area 2; 11. That means that the restricted area is identified for the central computer 1, and that not only facilitates the transmission of a code from the central computer 1 to the respective restricted area, it also increases the security in the system against unauthorized use.

[0032] According to one embodiment, the system can be used to ensure that, for example, the right people enter a meeting room. In that case, a person's transponder, in the form of an RFID circuit or a Bluetooth circuit in the mobile telephone of the person, is read by a communicator 12 at the door of the room. The communicator 12 transmits to the central computer 1 a code that is associated with the person's transponder. The central computer 1 transmits a temporary code to the mobile telephone 3 of the person, which mobile telephone sends the code onwards to the central computer 1 through the communicator 12. A circuit has in that way been

created, in which the central computer has information about the temporary code, the person's mobile telephone number coupled to that code that was initially read, and the name of the person.

[0033] According to another preferred embodiment, the code is used to encrypt information that is transmitted from the restricted area to the central computer. The code can in that way include an encryption key. That further increases the security against the unauthorized use of a code that has been read by eavesdropping.

[0034] According to a further preferred embodiment, the respective restricted area 2; 11 includes a reading arrangement in communicators 4; 12 in order to read biometric data of the user, and in order to cause the communicator in the respective restricted area 2; 11 to transmit biometric data to the central computer 1. Such biometric data is transmitted to the central computer 1 for comparison with reference data previously stored in the central computer, in order to further increase the security that it is the correct person that is using the radio terminal 3 or the computer 2. The reading arrangement 4; 12 for reading biometric data of the user can be a reading arrangement known per se of a suitable type, such as for reading fingerprints or the iris of the eye.

[0035] A number of embodiments have been described above. It is, however, clear that the invention can be varied, for example with respect to the location at which the circuit is initiated and started, and the number of different restrictive areas to be accessed and that that form the circuit can also be varied.

[0036] The present invention, therefore, is not to be seen as limited to the embodiments specified above, since the invention can be varied within the scope of the attached claims.